4

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/898,365	07/03/2001	Teng Pin Poo	1601457-0007	4356

7590 02/20/2007

White & Case, LLP
Attn: Patent Department
1155 Avenue of the Americas
New York, NY 10036

EXAMINER	
GELAGAY, SHEWAYE	
ART UNIT	PAPER NUMBER
2137	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/20/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/898,365	POO ET AL.	
	Examiner	Art Unit	
	Shewaye Gelagay	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 October 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14,16-20,23 and 24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14,16-20,23 and 24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/27/05, 2/24/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. In view of the Appeal Brief filed on 10/20/06, PROSECUTION IS HEREBY REOPENED. A new ground of rejection set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

2. Claims 1-14, 16-20 and 22-24 are pending.

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Response to Arguments

3. Applicant's arguments filed 10/20/06 have been considered but are moot in view of the new grounds of rejection. Appeal Brief Conference took place with conferee participants the examiner, a Primary Examiner and a Supervisory Examiner and it was

determined that the rejection under 35 U.S.C. 102 with new citation would have been more appropriate. A decision was made to reopen prosecution with proper citation. Therefore, the Office Rejection is amended accordingly.

4. In response to applicants argument that Bialick fails to teach or disclose "access to the non-volatile memory is granted to a user provided that the biometrics-based authentication module authenticates the user's identity and wherein access to the non-volatile memory is denied to the user otherwise". The examiner would like to point out Bilack teaches peripheral device with a non-volatile memory data storage device (figure 8, item 803) which can be accessed by using biometric authentication. Bilack teaches an access code such as a pin, password or biometrics has to be entered before a user is enabled to access data stored in a memory of the peripheral device. (col. 10, lines 45-col. 11, line 10)

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1, 2, 4, 5, 7, 8,10, 11, 13-14, 17, 18 and 20 are rejected under 35 U.S.C. 102(e) as being anticipated by Bialick et al. United States Letters Patent No. 6,088,802.

As per claim 1:

Bialick et al. teach a portable device comprising:

a microprocessor; and (Figure 8, item 801)

a non-volatile memory coupled to the microprocessor; (Figure 8, item 803; Col. 16, lines 10-16) and

a biometrics-based authentication module coupled to and controlled by the microprocessor, wherein access to the non-volatile memory is granted to a user provided that the biometrics-based authentication module authenticates the user's identity and wherein access to the non-volatile memory is denied to the user otherwise. (Col. 10, line 45-Col. 11, line 10; Col. 14, line 10-col. 15, line 23; Col. 16, lines 10-16)

As per claim 2:

The rejection of claim 1 is incorporated and further Bialick et al. disclose the biometrics-based authentication module is a fingerprint authentication module. (Col. 14, lines 26-28)

As per claim 4:

The rejection of claim 1 is incorporated and further Bialick et al. disclose the biometrics-based authentication module comprises a biometrics sensor fitted on one surface of the portable device. (Col. 14, lines 48-49; Col. 14, line 59-Col. 15, line 7)

As per claim 5:

The rejection of claim 1 is incorporated and further Bialick et al. disclose a non-volatile memory capable or storing biometrics information usable for authentication. (Figure 8, item 803; Col. 14, lines 57-58; Col. 16; lines 10-11)

As per claim 7:

Bialick et al. disclose a portable device comprising:

a bus; (Figure 6, item 609)

a microprocessor coupled to the bus; (Figure 8, item 801)

a non-volatile memory coupled to the bus (Figure 8, item 803; Col. 16, lines 10-15); and

a biometrics-based authentication module coupled to the bus, wherein under the control of the microprocessor the biometrics-based authentication module is configured to (1) capture a first biometrics marker; (Col. 14, lines 55-56) (2) store the first biometrics marker in the non-volatile memory; (Col. 14; lines 57-58) (3) capture a second biometrics marker; (Col.14; line 54) and (4) determine whether the second biometrics marker can be authenticated against the first biometrics marker; (Col.14; line 54)and wherein microprocessor is configured to disable access to the non-volatile memory upon a determination of authentication failure by the biometrics-based authentication module. (Col. 10, line 45-Col. 11, line 10; Col. 14, line 10-col. 15, line 23; Col. 16, lines 10-16)

As per claim 8:

The rejection of claim 7 is incorporated and further Bialick et al. disclose the biometrics-based authentication module is a fingerprint authentication module. (Col. 14, lines 26-28)

As per claim 10:

The rejection of claim 7 is incorporated and further Bialick et al. disclose the biometrics-based authentication module is structurally integrated with the portable device in a unitary construction and comprises a biometrics sensor being disposed on one surface of the portable device. (Col. 14, lines 48-49; Col. 14, line 59-Col. 15, line 7)

As per claim 11:

The rejection of claim 7 is incorporated and further Bialick et al. disclose a portable device, wherein the non-volatile memory comprises flash memory. (Figure 8, item 803)

As per claim 13:

The rejection of claim 7 is incorporated and further Bialick et al. disclose a portable device, wherein the microprocessor is configured to direct the biometrics-based authentication module to capture and store the first biometrics marker provided that no biometrics marker has been stored in the non-volatile memory. (Col. 14, lines 55-58)

As per claim 14:

The rejection of claim 7 is incorporated and further Bialick et al. disclose a portable device, wherein the microprocessor is configured to enable access to the non-volatile memory upon a determination of authentication success by the biometrics-

based authentication module. (Col. 10, line 45-Col. 11, line 10; Col. 14, line 10-col. 15, line 23; Col. 16, lines 10-16)

As per claim 17:

Bialick et al. teach a biometrics-based authentication method implemented using a portable device, the method comprising the steps of: (a) obtaining a first biometrics marker from a user with a biometrics sensor installed on the portable device; (Col.14; line 54) (b) retrieving a registered biometrics marker from a non-volatile memory of the portable device, the registered biometrics marker having been stored therein during a registration process; (Col. 14; lines 57-58) (c) comparing the first biometrics marker against the registered biometrics marker; (Col. 14; lines 54-56) (d) denying the user access to the non-volatile memory provided that a match is not identified in said step (c); (Col. 10, line 45-Col. 11, line 10; Col. 14, line 10-col. 15, line 23; Col. 16, lines 10-16) (e) signaling an authentication success provided that a match is identified in said step (c). (Col. 10, line 45-Col. 11, line 10; Col. 14, line 10-col. 15, line 23; Col. 16, lines 10-16)

As per claim 18:

The rejection of claim 17 is incorporated and further Bialick et al. disclose biometrics-based access control method, wherein the registered biometrics marker is a fingerprint. (Col. 14, lines 26-28)

As per claim 20:

The rejection of claim 17 is incorporated and further Bialick et al. disclose the step of denying the user access to the restricted resource provided that a match is not

identified in said step (c). (Col. 10, line 45-Col. 11, line 10; Col. 14, line 10-col. 15, line 23; Col. 16, lines 10-16)

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

8. Claims 6, 12, 16, 19 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bialick et al. United States Letters Patent No. 6,088,802.

As per claim 6:

Bialick et al. teach all the subject matter as described above. Bialick et al. further disclose the peripheral device driver can be implemented so that the user must successfully enter an acceptable access code (e.g., a password or PIN) before the user is enabled to use the peripheral device. (Col. 10; lines 45-47) Not explicitly disclosed by Bialick et al. is that, the microprocessor is configured to provide a bypass mechanism for authentication upon a determination of authentication failure by the biometrics-based authentication module. However, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Bialick et al.'s method to include a microprocessor that is configured to provide a bypass mechanism for authentication upon a determination of authentication failure by the biometrics-based authentication module. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so by the suggestion provided by Bialick et al., in order to use the security functionality, thus enabling a layer of security that protects the integrity of the restricted resources.

As per claim 12:

Bialick et al. teach all the subject matter as described above. Bialick et al. further disclose the peripheral device further configured to encrypt the first biometrics marker before storing the first biometrics marker in the non-volatile memory.

However, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Bialick et al.'s method to include further configured to encrypt the first biometrics marker before storing the first biometrics marker in the non-volatile memory. This modification would have been obvious

because a person having ordinary skill in the art would have been motivated to do so by the suggestion provided by Bialick et al., in order to enhance the security of the biometrics-based access control method.

As per claim 16:

Bialick et al. teach all the subject matter as described above. Bialick et al. further disclose the peripheral device driver can be implemented so that the user must successfully enter an acceptable access code (e.g., a password or PIN) before the user is enabled to use the peripheral device. (Col. 10; lines 45-47) Not explicitly disclosed by Bialick et al. is that, a bypass mechanism for authentication is provided upon a determination of authentication failure by the biometrics-based authentication module.

However, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Bialick et al.'s method to include a bypass mechanism for authentication is provided upon a determination of authentication failure by the biometrics-based authentication module. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so by the suggestion provided by Bialick et al., in order to use the security functionality, thus enabling a layer of security that protects the integrity of the restricted resources.

As per claim 19:

Bialick et al. teach all the subject matter as described above. Bialick et al. further disclose the peripheral device can be used to encrypt or decrypt data stored. Not

explicitly disclosed by Bialick et al. is that, the registered biometrics marker is stored in an encrypted format.

However, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Bialick et al.'s method to include the registered biometrics marker is stored in an encrypted format. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so by the suggestion provided by Bialick et al., in order to enhance the security of the biometrics-based access control method.

As per claim 22:

Bialick et al. teach all the subject matter as described above. Bialick et al. further disclose the peripheral device driver can be implemented so that the user must successfully enter an acceptable access code (e.g., a password or PIN) before the user is enabled to use the peripheral device. (Col. 10; lines 45-47) Not explicitly disclosed by Bialick et al. is that, providing the user with a bypass authentication procedure provided that a match is not identified in said step (c).

However, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Bialick et al.'s method to include providing the user with a bypass authentication procedure provided that a match is not identified in said step (c). This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so by the suggestion provided by Bialick et al., in order to use the security functionality, thus enabling a layer of security that protects the integrity of the restricted resources.

9. Claims 3 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bialick et al. United States Letters Patent No. 6,088,802 and in view of Bjorn United States Letters Patent No. 6,799,275 .

As per claim 3:

Bialick et al. teach all the subject matter as described above. In addition, Bialick et al. disclose a communication interfaces, such as a smart card interface, a serial interface or a SCSI interface or an IDE interface. Not explicitly disclosed by Bialick et al. is that the portable device, further comprising a universal serial bus (USB) connector for coupling with another USB-compliant device.

Bjorn in analogous art, however, teaches a device further comprising a universal serial bus (USB) connector for coupling with another USB-compliant device. (Col. 2, lines 59-60; the digital connection is a data bus, which conforms to a universal serial bus (USB) standard.)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Bialick et al. to include a device further comprising a universal serial bus (USB) connector for coupling with another USB-compliant device. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Bjorn, in order to provide a faster transfer of digitized image.

As per claim 9:

Bialick et al. teach all the subject matter as described above. In addition, Bialick et al. disclose a communication interfaces, such as a smart card interface, a serial

interface or a SCSI interface or an IDE interface. Not explicitly disclosed by Bialick et al. the portable device comprising a universal serial bus (USB) device controller coupled to the bus and a USB connector coupled to the bus, such that the portable device is capable of communicating with a host platform via the USB connector.

Bjorn in analogous art, however, teaches a device comprising a universal serial bus (USB) device controller coupled to the bus and a USB connector coupled to the bus, such that the portable device is capable of communicating with a host platform via the USB connector. (Col. 2, lines 59-60; the digital connection is a data bus, which conforms to a universal serial bus (USB) standard.)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Bialick et al. to include a device comprising a universal serial bus (USB) device controller coupled to the bus and a USB connector coupled to the bus, such that the portable device is capable of communicating with a host platform via the USB connector. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Bjorn, in order to provide a faster transfer of digitized image.

10. Claims 23-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bialick et al. United States Letters Patent No. 6,088,802 and in view of Estakhri et al. (hereinafter Estakhri) United States Letters Patent No. 6,385,667.

As per claim 23:

Bialick teaches a unitary portable data storage device having biometrics capability the device comprising:

housing; (Figure 3a)

a fingerprint module, at least a portion of which is housed within the housing, the fingerprint module including a sensor disposed on an exterior surface of the housing; (Col. 14, lines 21-67)

a memory including non-volatile memory, the memory housed within the housing and coupled to the fingerprint module and is configured to store at least one fingerprint template as well as user data; (Figure 8, item 803; Col. 14; lines 10-58 and Col. 16, lines 10-15)

a memory controller housed within the housing and coupled to the memory, the memory controller controlling access to the memory; (Figure 8, item 801)

wherein the fingerprint module is configured to (1) receive a fingerprint sample from a user placing a finger on the sensor; (Col. 14, lines 55-56) (2) compare the fingerprint sample with said at least one finger template; (Col. 10, line 45-Col. 11, line 10; Col. 14, line 10-col. 15, line 23; Col. 16, lines 10-16) and (3) reject a request from the user to access the user data stored in the memory provided that the comparison in said step (2) results in no match. (Col. 10, line 45-Col. 11, line 10; Col. 14, line 10-col. 15, line 23; Col. 16, lines 10-16)

In addition, Bialick et al. disclose a communication interfaces, such as a smart card interface, a serial interface or a SCSI interface or an IDE interface. Not explicitly disclosed by Bialick et al. a USB plug integrated into the housing without an intervening

cable and capable of coupling the unitary portable data storage device directly to a USB socket on a host computer and a USB device controller housed within the housing, the USB device controller enabling the unitary portable data storage device to communicate with the host computer via the USB protocol.

Estakhri in analogous art, however, teaches a USB plug integrated into the housing without an intervening cable and capable of coupling the unitary portable data storage device directly to a USB socket on a host computer; (Figure 3, element 300, element 314). and a USB device controller housed within the housing, the USB device controller enabling the unitary portable data storage device to communicate with the host computer via the USB protocol. (Figure 3, element 300, element 314, element 335, element 330; Col. 5, lines 19-51)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Bialick et al. to include a USB plug integrated into the housing without an intervening cable and capable of coupling the unitary portable data storage device directly to a USB socket on a host computer and a USB device controller housed within the housing, the USB device controller enabling the unitary portable data storage device to communicate with the host computer via the USB protocol. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Estakhri, (Col. 1, lines 16-17) in order to provide an interface facilitating user-friendly connectivity and a faster transfer of digitized image.

As per claim 24:

Bialick and Estakhri disclose all the subject matter as discussed above. In addition Estakhri further discloses a device wherein at least a portion of the USB plug protrudes from the housing to facilitate direct coupling of the unitary portable data storage device to the USB socket of a computer. (Figure 3, item 314)

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shewaye Gelagay SG

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100